Algebra I, Fall 2016

Solutions to Problem Set 9

1. Since IM is a R-submodule of M, M/IM is a R-module. We first show that as R-modules M/IM and $M \otimes_R R/I$ are isomorphic. There is a bilinear map $M \otimes_R R/I \to M/IM$ which sends $(m, r+I)$ to $rm + IM$. This induces a R-homomorphism $\phi : M \otimes_R R/I \to M/IM$. There is also a R-homomorphism $\psi : M/IM \to M \otimes_R R/I$ which sends $m + IM$ to $m \otimes (1 + I)$. ψ is well-defined since if $m \in IM$, $m = r_1m_1 + \cdots + r_km_k$with $r_i \in I$, and so $\psi(m) = (r_1m_1 + \cdots + r_km_k) \otimes (1 + I) = r_1(m_1 \otimes (1 + I)) + \cdots + r_k(m_k \otimes (1 + I)) = m_1 \otimes (r_1 + I) + \cdots + m_k \otimes (r_k + I) = 0$. The R-homomorphisms ϕ and ϕ are inverse to each other and therefore, ϕ is an isomorphism.

Now to show ϕ is also an isomorphism of R/I-modules, it is enough to show ϕ respects multiplication with elements of R/I. We have $\phi((r+I)(m \otimes (s+I))) = \phi(m \otimes (rs + I)) = rsm + IM = (r + I)(sm + IM) = (r + I)\phi(m \otimes (s + I))$.

2. (a). Pick $x \in M$. By our choice of s_1, $p^{s_1}x = 0$ since x is a linear combination of the m_i. Let r be the minimum positive integer such that $p^r x \in N$. Then $r \leq s_1$. We have $p^r x = \lambda m_1$ for some $\lambda \in R$, and $p^{s_1-r}p^r x = 0$, so $p^{s_1-r}\lambda m_1 = 0$. Hence p^r divides λ, since by part (i) of Question 3, $\gcd(p^{s_1}, p^{s_1-r}\lambda)m_1 = 0$. Write $\lambda = p^r\beta$. Then $p^r x = \lambda m_1 = p^r\beta m_1$, so $p^r(x-\beta m_1) = 0$. Set $y := x-\beta m_1$. We claim that y has the desired property. Clearly $y+N = x+N$. Also, if $p^s y \in N$, then $p^s x \in N$, so $s \geq r$ by our choice of r. Therefore $p^s y = p^s(x - \beta m_1) = 0$. Note that this shows more generally that if $\eta \in R$ is such that $\eta y \in N$, then $\eta y = 0$. The reason is that $\eta y \in N$ implies $\eta(y+N) = 0$, and since $p^r(y+N) = 0$, by question 3 part (i) we have $\gcd(\eta, p^r)(y + N) = 0$, and since $\gcd(\eta, p^r)$ is of the form p^s for some s, we conclude that $p^s(y + N) = 0$, so $p^s y \in N$. Therefore, $p^s y = 0$, and so $\eta y = 0$.

(b) We use induction on the number k of a set of generators. If $k = 1$, there is nothing to prove. Assume the statement is true for $k-1$. and $M =<$

$m_1, \ldots, m_k >$ be as in part (a). Then there is a short exact sequence of R-modules

$$0 \to N \to M \to M/N \to 0$$

and M/N is generated by $k-1$ elements so there is an isomorphism

$$\phi : M_1 \oplus \cdots \oplus M_n \to N/M$$

where M_i is an R-modules which is generated by an element $a_i \in M_i$. For each i, let x_i be such that $\phi(0, \ldots, a_i, \ldots, 0) = x_i + N$, and let y_i be the corresponding y as in part (a). Define now a R-homomorphism

$$\psi : M_1 \oplus \cdots \oplus M_n \oplus N \to M$$

by $\psi(\mu_1 a_1, \ldots, \mu_n a_n, y) = \mu_1 y_1 + \cdots + \mu_n y_n + y$. Then part a shows that this map is well-defined: if $(\mu_1 a_1, \ldots, \mu_n a_n, y) = (\eta_1 a_1, \ldots, \eta_n a_n, y)$, then $(\mu_i - \eta_i)a_i = 0$, for every $1 \le i \le n$ so $(\mu_i - \eta_i)x_i \in N$, so $(\mu_i - \eta_i)y_i \in N$, so $(\mu_i - \eta_i)y_i = 0$. Therefore, $\mu_i y_i = \eta_i y_i$. It is clear that ψ is one-to-one and onto and is therefore an isomorphism.

3. (i) There are $x, y \in R$ such that $\gcd(a,b) = xa + yb$. Hence $\gcd(a,b)m = xam + ybm = 0$.

(ii) There is a homomorphism $\phi : M_b \oplus M_c \to M_a$ which sends (m_1, m_2) to $m_1 + m_2$. We show ϕ is bijective. ϕ is injective since if $\phi(m_1, m_2) = 0$, $m_1 = -m_2$, so $m_1 \in M_b \cap M_c$, so by part (a) $m_1 = 0$ and hence $m_2 = 0$. To show ϕ is surjective note that there are $x, y \in R$ such that $1 = xb + yc$, so $m = xbm + ycm$. Let $m_1 = ycm$ and $m_1 = xbm$. If $am = 0$, then $bm_1 = 0$ and $cm_2 = 0$, so $(m_1, m_2) \in M_b \oplus M_c$ and $\phi(m_1, m_2) = m$.

(iii) Let s be the smallest positive integer such that $p^s m = 0$, and let N be the submodule generated of M by m. We show $N \simeq R/(p^s)$. There is a homomorphism $\psi : R/(p^s) \to N$ which sends $r + (p^s)$ to rm. We show ψ is well-defined and injective: if $r \in (p^s)$, then $r = r'p^s$, so $rm = r'p^s m = 0$. And conversely, if $rm = 0$, then by part (i) $\gcd(r, p^s)m = 0$, but $\gcd(r, p^s) = p^{s'}$ with $s' \le s$, so by our assumption on s, $s' = s$ and $r \in (p^s)$. The map ψ is clearly surjective, so it is an isomorphism.

4. Let $K = F(\alpha^2)$. Then we have $F \subseteq K \subseteq E$. If $\alpha \in K$, then $E = K = F(\alpha^2)$. Otherwise α is algebraic of degree 2 over K. Therefore $[E : K] = 2$, but then $[E : F] = [E : K][K : F] = 2[K : F]$ contradicting the assumption that $[E : F]$ is an odd extension.